

Decoy-State Quantum Key Distribution with Nonclassical Light Generated in a One-dimensional Waveguide

Huaixiu Zheng*, Daniel J. Gauthier, and Harold U. Baranger†

Department of Physics, Duke University, P. O. Box 90305, Durham, North Carolina 27708, USA

**Corresponding author: hz33@duke.edu*

†Corresponding author: baranger@phy.duke.edu

Compiled October 4, 2012

We investigate a decoy-state quantum key distribution (QKD) scheme with a sub-Poissonian single-photon source, which is generated on demand by scattering a coherent state off a two-level system in a one-dimensional waveguide. We show that, compared to coherent state decoy-state QKD, there is a two-fold increase of the key generation rate. Furthermore, the performance is shown to be robust against both parameter variations and loss effects of the system. © 2012 Optical Society of America

OCIS codes: 270.5290, 270.5565, 270.5568

Quantum key distribution (QKD), which allows two distant users, Alice and Bob, to share a secret key with security guaranteed by principles of quantum physics, is the first commercially available application of quantum information science. The first QKD protocol, BB84 [1], proposes to use an ideal single-photon source, which is still beyond the current technology despite tremendous experimental effort worldwide. Hence, most QKD experiments use weak coherent states (WCS) from attenuated lasers as a photon source [2–8]. Two drawbacks come with the WCS: the multiphoton and the vacuum components. The vacuum content limits Bob’s detection rate, and hence leads to a shorter maximal distance. The multiphoton component makes QKD vulnerable to the photon number splitting attack, where the eavesdropper (Eve) can suppress single-photon signals and split multiphoton signals, keeping one copy and sending one copy to Bob. This way, Eve obtains the full information without being detected, and the unconditional security breaks down. The decoy state method was proposed to beat such attacks [9]: Alice prepares additional decoy states, and learns about the eavesdropping from their transmission. Recently, alternative light sources, including spontaneous parametric down-conversion [10] and heralded single-photons [11], have been used in decoy-state QKD.

In this paper, we combine the decoy-state method with a sub-Poissonian single-photon source generated on demand by scattering in a waveguide. We find that there is a substantial increase in the key generation rate and maximal transmission distance compared to both WCS and heralded single-photon decoy-state QKD. Furthermore, the performance is robust against either parameter variation or loss in the system, making it a promising candidate for future QKD systems.

Recently, strong coupling between light and matter has been achieved in a variety of one-dimensional (1D) waveguide-QED systems [12–15]. This great experimental progress has stimulated extensive theoretical study of nonlinear effects in such systems for the purpose of quantum information processing [16–21]. One applica-

tion is to generate nonclassical light by sending a coherent state into a 1D waveguide which is side-coupled to a quantum nonlinear element, such as a two-level system (2LS) [14, 22]. The nonlinearity of the quantum element leads to a distinct difference between multiphoton and single-photon scattering. For example, when two photons interact with a 2LS simultaneously, the 2LS will only be able to absorb one photon and hence the pair will have a high transmission probability. This is confirmed in Ref. 22, where we show that the photon number statistics of the transmitted field follow a super-Poissonian distribution. Here, we focus on the reflected field, which has sub-Poissonian statistics.

Figure 1 shows the probabilities P_n to measure n -photon states in the reflected field after scattering a coherent state off the 2LS. We will call such a photon source the “2LS source”. The input coherent state has mean photon number $\bar{n} = 1$. We take a Gaussian wavepacket with central frequency on resonance with the 2LS and root-mean-square spectral width σ . The excited state of the 2LS decays into the waveguide mode at rate Γ and into other modes at rate Γ' . For now, we set the loss rate $\Gamma' = 0$, returning to consider the effect of loss later. For comparison, we also show P_n (dashed line) of a coherent state with the same mean photon number as the reflected field. It is remarkable that, for the full parameter range, the reflected field has higher single-photon and lower vacuum and multiphoton content than the coherent state. In the insert of Fig. 1, we show that the multiphoton content is strongly suppressed at $\Gamma = 2\sigma$. This is in agreement with the antibunching behavior of microwave photons observed in a recent experiment [14], and is the key to increasing the key generation rate.

Now, we discuss the decoy-state method with light sources, including weak coherent states, a heralded single-photon source (HSPS), and the 2LS source (2LSS). The secure key generation rate is given by [23]

$$R \geq q\{-Q_s f(E_s) H_2(E_s) + Q_1[1 - H_2(e_1)]\}, \quad (1)$$

where the efficiency q is 1/2 for the Bennett-Brassard

1984 (BB84) protocol, $f(E_s)$ is the error correction efficiency (we use $f = 1.22$ [24]), Q_s and E_s are the overall gain and error rate of signal states, respectively, Q_1 and e_1 are the gain and error rate of single-photon states, respectively, and $H_2(x)$ is the binary Shannon information function: $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

In Eq. (1), while Q_s and E_s are measurable quantities in experiments, Q_1 and e_1 are unknown variables. Q_s and E_s are given by

$$Q_s = \sum_{n=0}^{\infty} p_n^s Y_n, \quad E_s = \frac{1}{Q_s} \sum_{n=0}^{\infty} p_n^s Y_n e_n, \quad (2)$$

where p_n^s is the n -photon probability of signal states, e_n is the error rate of an n -photon state, and Y_n is the n -photon yield, i.e., the conditional probability of a click on Bob's side given that Alice has sent an n -photon state.

To generate a lower bound on the key generation rate, we have to estimate a lower bound of Q_1 (or equivalently Y_1 as $Q_1 = p_1^s Y_1$) and an upper bound of e_1 . Estimating the lower bound Y_1^l and the upper bound e_1^u based solely on Eq. (2) unavoidably underestimates the secure key generation rate due to the lack of enough information about the transmission channel. The decoy-state idea [9] is a clever way to obtain additional channel information by sending decoy states in addition to the signal states. The decoy states are used to detect eavesdropping, but not for key generation. By measuring the transmission of the decoy states, Alice and Bob have another set of constraints

$$Q_d = \sum_{n=0}^{\infty} p_n^d Y_n, \quad E_d = \frac{1}{Q_d} \sum_{n=0}^{\infty} p_n^d Y_n e_n, \quad (3)$$

where Q_d and E_d are the measured overall gain and error rate of decoy states, respectively. Because Eve has no way to distinguish an n -photon decoy state from an n -photon signal state, the yield Y_n and the error rate e_n are the same for both the decoy and signal states.

For our numerical simulation, we use the channel model in Ref. 25 to calculate the experimental parameters Q_s , E_s , Q_d , and E_d . In this model, the yield is $Y_n = 1 - (1 - Y_0)(1 - \eta)^n$, where Y_0 is the background rate and η is the overall transmittance given by $\eta = t_{AB}\eta_{Bob}$, where $t_{AB} = 10^{-\alpha\ell/10}$ is the channel transmittance and η_{Bob} is the detection efficiency on Bob's side. Here, α is the loss coefficient and ℓ is the transmission distance. The error rate is given by $e_n = [e_0 Y_0 + e_d(Y_n - Y_0)]/Y_n$, where e_d is the probability that a photon hits the wrong detector and e_0 is the error rate of the background. We use the experimental parameters in Ref. 2: $\alpha = 0.21\text{dB/km}$, $e_d = 3.3\%$, $Y_0 = 1.7 \times 10^{-6}$, $e_0 = 0.5$, and $\eta_{Bob} = 0.045$.

We apply the linear programming method [26] to estimate Y_1^l and e_1^u from Eqs. (2) and (3). This method is applicable to light sources with general number statistics. We use two decoy states—the vacuum and a weak decoy state. For the weak coherent states, the key generation rate is optimized in terms of the mean photon

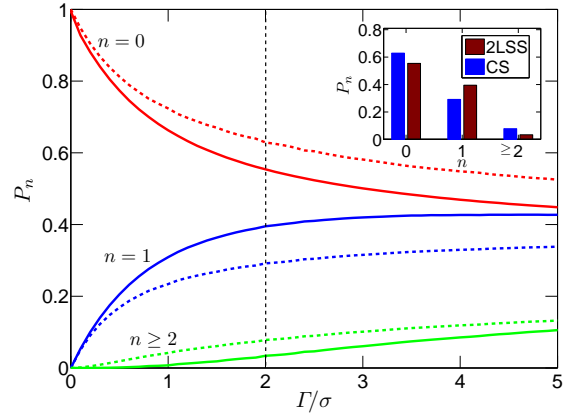


Fig. 1. Nonclassical light source. The number statistics P_n of the 2LS source (2LSS, solid), and a coherent state (CS, dashed) of the same mean photon number as a function of Γ/σ . Insert: P_n at $\Gamma/\sigma = 2$. Here, we set $\Gamma' = 0$.

number in both the signal and decoy states. For the heralded single-photons, we use the number statistics from Ref. 11. For the 2LS source, the signal and decoy states are generated by scattering coherent states of $\bar{n} = 1$ and $\bar{n} = 0.02$, respectively. We choose $\sigma = \Gamma/2$.

Figure 2 shows the resulting key generation rate. With the same experimental parameters and estimation technique, our scheme using the 2LS source obtains a two-fold increasing of key generation rate compared to the WCS method. The maximal transmission distance is increased as well. In addition, our scheme also outperforms the HSPS scheme. Such a performance enhancement is due to the reduced vacuum and multiphoton contents, as shown in Fig. 1.

Next, we investigate the robustness of our scheme with respect to the variation of system parameter Γ/σ . As shown in Fig. 3(a), the key generation rate gradually converges as Γ/σ increases. In particular, the insert shows that the maximal transmission distance (ℓ_{\max}) has little

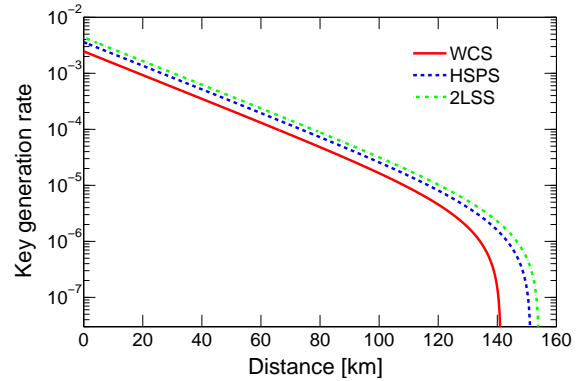


Fig. 2. Key generation rate with different light sources: weak coherent state (WCS), heralded single-photon source (HSPS), and 2LS source (2LSS) with $\Gamma/\sigma = 2$ and $\Gamma' = 0$

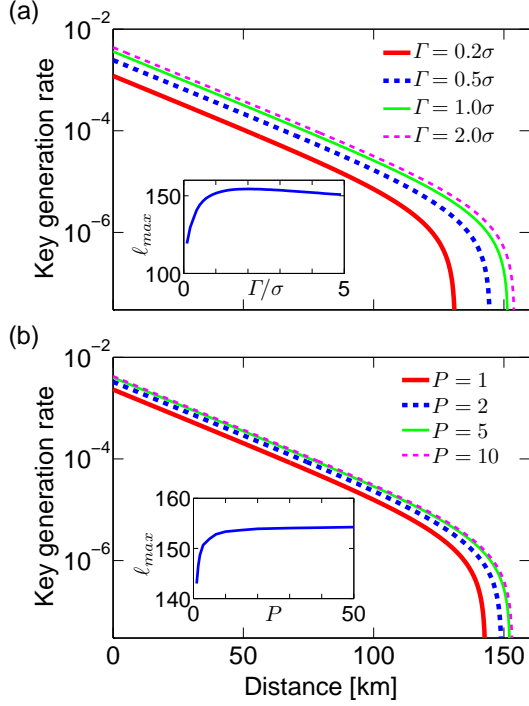


Fig. 3. Key generation rate of 2LS sources with parameter variation and loss: (a) $\Gamma = 0.2\sigma, 0.5\sigma, \sigma, 2\sigma$. Insert: maximal transmission distance (ℓ_{\max}) as a function Γ/σ . $\Gamma' = 0$; (b) $P = 1, 2, 5, 10$. Insert: ℓ_{\max} as a function of P . We choose $\Gamma = 2\sigma$.

change for $\Gamma/\sigma \geq 1$.

Figure 3(b) shows the effect of loss on the system performance. We fix $\Gamma = 2\sigma$ and choose different loss rates Γ' of the 2LS. We define an effective Purcell factor $P = \Gamma/\Gamma'$ to quantify the strength of loss: $P \rightarrow 0$ means large loss and $P \rightarrow \infty$ means negligible loss. In Fig. 3(b), we observe that, as P increases, the key generation rate increases and converges. It is evident that, for $P \geq 10$, the performance is very reliable against loss as shown in the insert. Given that values of P as large as 30 have already been achieved in a recent experiment [27], our scheme can be practically useful for quantum key distribution.

This work was supported by US NSF Grant No. PHY-10-68698. H.Z. is supported by a John T. Chambers Fellowship from the Fitzpatrick Institute for Photonics at Duke University.

References

- C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
- G. Gobby, Z. L. Yuan, and A. J. Shields, *Appl. Phys. Lett.* **84**, 3762 (2004).
- Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Phys. Rev. Lett.* **96**, 070502 (2006).
- C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, *Phys. Rev. Lett.* **98**, 010505 (2007).
- T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, et al., *Phys. Rev. Lett.* **98**, 010504 (2007).
- D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, *Phys. Rev. Lett.* **98**, 010503 (2007).
- D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, et al., *New J. Phys.* **11**, 045009 (2009).
- H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- W.-Y. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005); X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).
- Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **99**, 180503 (2007).
- Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, *Phys. Rev. Lett.* **100**, 090501 (2008).
- J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gérard, *Nat. Photon.* **4**, 174 (2010).
- O. Astafiev, A. M. Zagorskin, A. A. A. Jr., Y. A. Pashkin, T. Yamamoto, K. Inomata, Y. Nakamura, and J. S. Tsai, *Science* **327**, 840 (2010).
- I.-C. Hoi, C. M. Wilson, G. Johansson, T. Palomaki, B. Peropadre, and P. Delsing, *Phys. Rev. Lett.* **107**, 073601 (2011).
- A. Laucht, S. Pütz, T. Günthner, N. Hauke, R. Saive, S. Frédérick, M. Bichler, M.-C. Amann, A. W. Holleitner, M. Kaniber, et al., *Phys. Rev. X* **2**, 011014 (2012).
- D. E. Chang, A. S. Sørensen, E. A. Demler, and M. D. Lukin, *Nature Phys.* **3**, 807 (2007).
- J.-T. Shen and S. Fan, *Phys. Rev. Lett.* **98**, 153003 (2007); *Phys. Rev. A* **76**, 062709 (2007).
- E. Rephaeli, S. E. Kocabas, and S. Fan, *Phys. Rev. A* **84**, 063832 (2011).
- D. Roy, *Phys. Rev. Lett.* **106**, 053601 (2011).
- P. Kolchin, R. F. Oulton, and X. Zhang, *Phys. Rev. Lett.* **106**, 113601 (2011).
- H. Zheng, D. J. Gauthier, and H. U. Baranger, *Phys. Rev. Lett.* **107**, 223601 (2011); *Phys. Rev. A* **85**, 043832 (2012).
- H. Zheng, D. J. Gauthier, and H. U. Baranger, *Phys. Rev. A* **82**, 063816 (2010).
- D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, *Quantum Inf. Comput.* **4**, 325 (2004).
- G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
- X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Phys. Rev. A* **72**, 012326 (2005).
- T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms* (MIT Press and McGraw-Hill, New York, 2009), 3rd ed.
- M. H. Mikkelsen, private communication (2012).